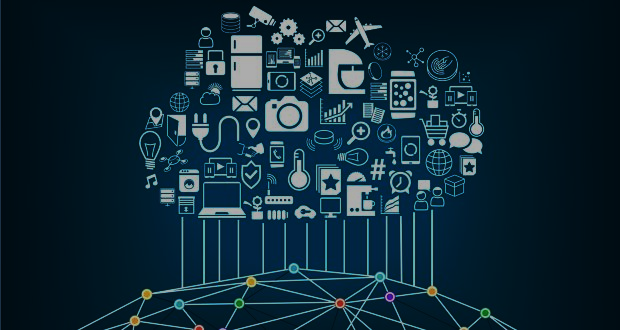




**Google for Log**



What does Splunk do?

**Run the business in real-time.**

**Make machine data accessible, usable and valuable to everyone to make operation more intelligent such as.**

Real time business insights

Live dashboards, Event correlation, Monitoring and alerting, Performance Issues, Transaction levels, SLA tracking

Search and Investigation

## Data drilldown, “Needle in a haystack”, Incident investigations

New Class of data for business analysis

Baseline and thresholds, Trending

Operational Visibility

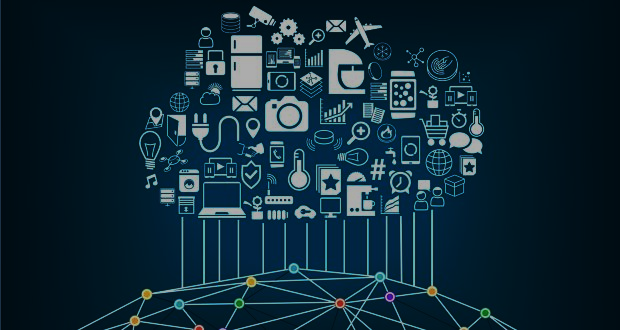
Operational insights, Historical patterns, Compliance reports

Proactive Monitoring

Root cause analysis/ troubleshooting

Enrich machine data with structured data

Dashboard



What does Splunk provide?

**Common interface of all IT data and you can perform**

Operational Intelligence

Search

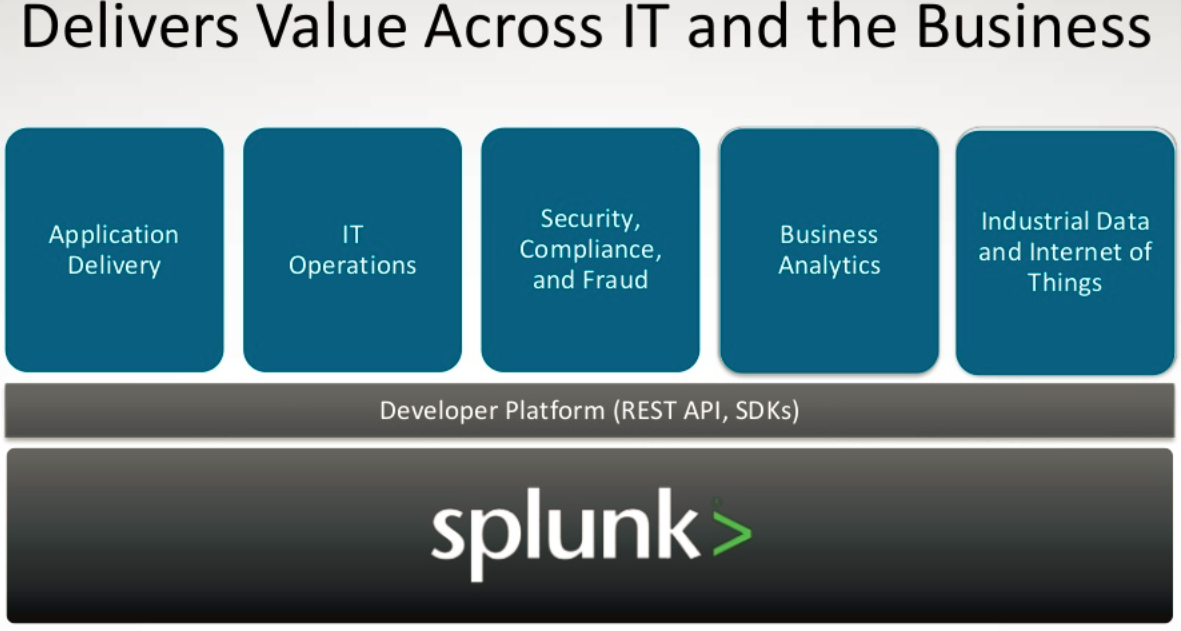
Correlation of disparate data in single tool across all technologies

**Quicker** – Root cause analysis

**Increases** – Situational awareness

**Lower**– Business Risk

Deliver values across IT and Business

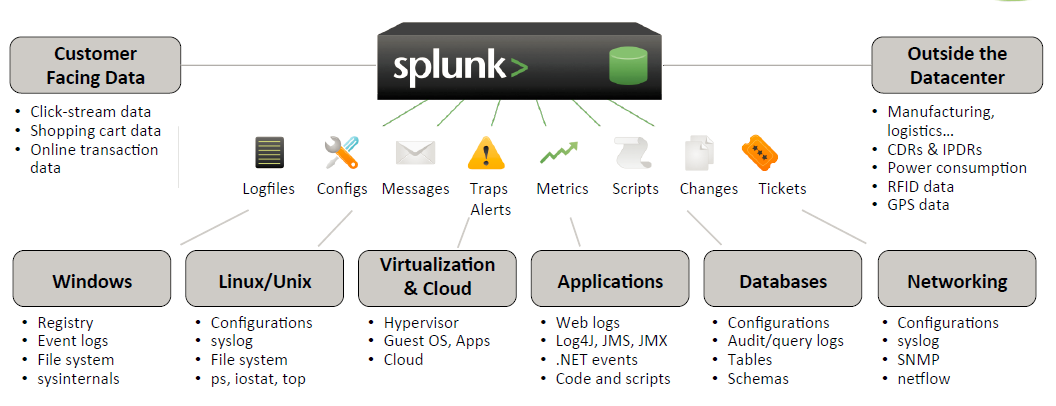


Alert

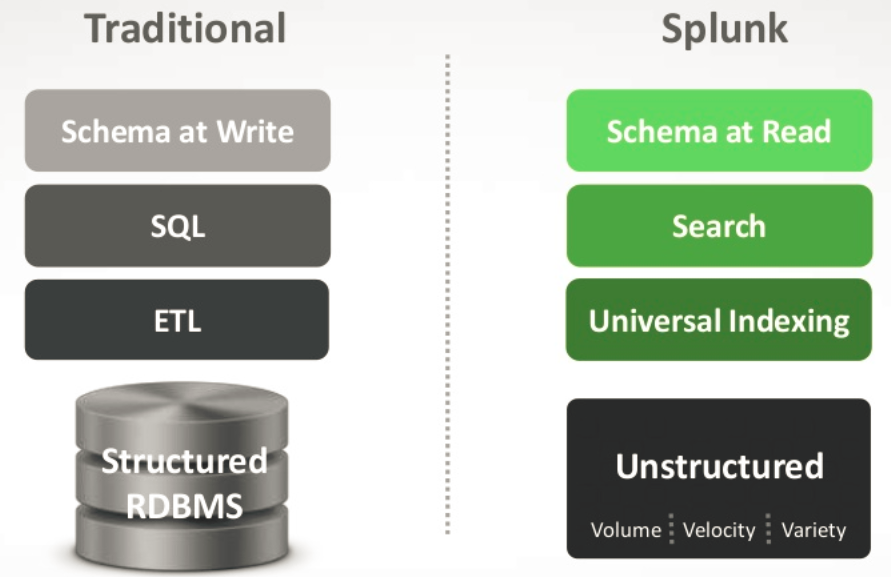
Report

Share

What can be indexed?



DB?



Data highly structured and so the database

Inflexible schema, long deployment cycle

Financial records, manufacturing and logisical information, personnel data

Time series unstructured data, with no predefined schema

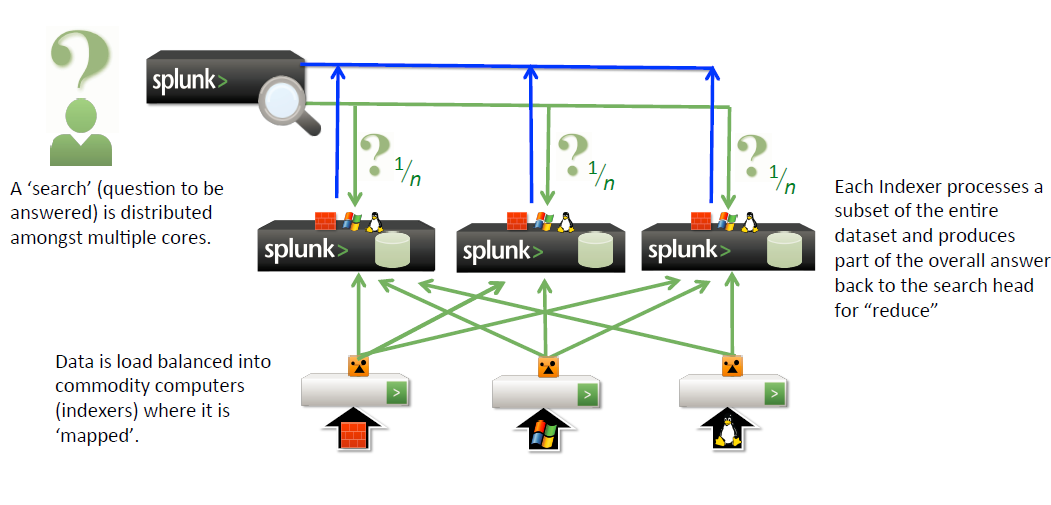
Generated by all IT systems, non-standard data, unpredictable formats

Massive volume; fast naviga6on and correlation paramount

How search works?

Using distributed search using [Map Reduce](https://en.wikipedia.org/wiki/MapReduce)

## MapReduce is a software framework introduced by Google in 2004 to support distributed compu6ng on large data sets on clusters of computers. - Wikipedia



How helps in pre-sales or improving customer service

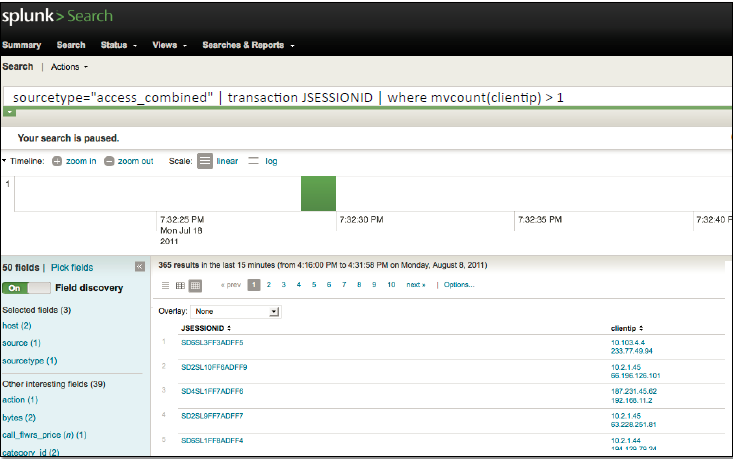
* Gain visibility into pre-order sales process across different selling points
* Get real-time sales insight by store and customer type
* Analyze transaction volums across different sales channels
* Perform pre-order customer segments analysis

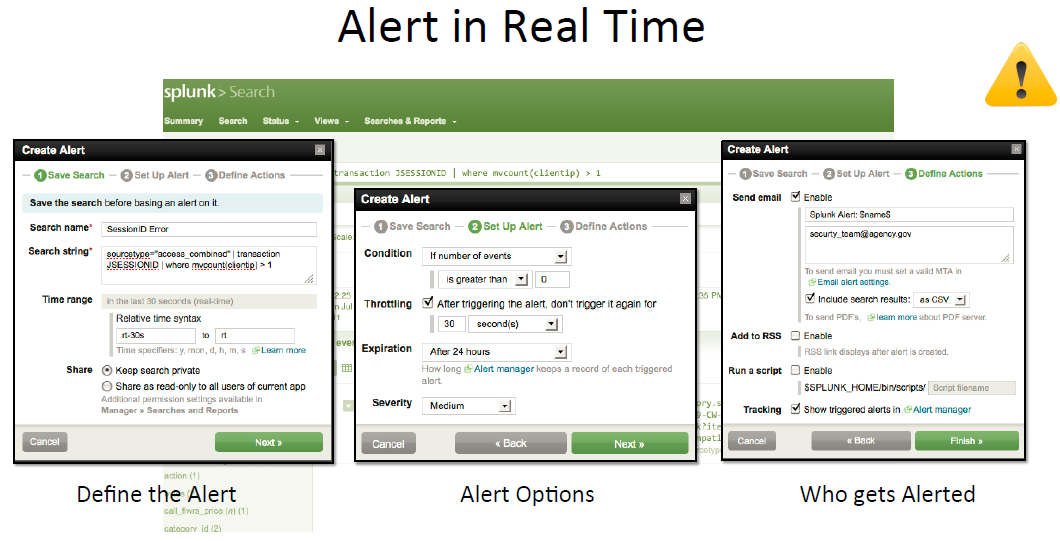
Objects>

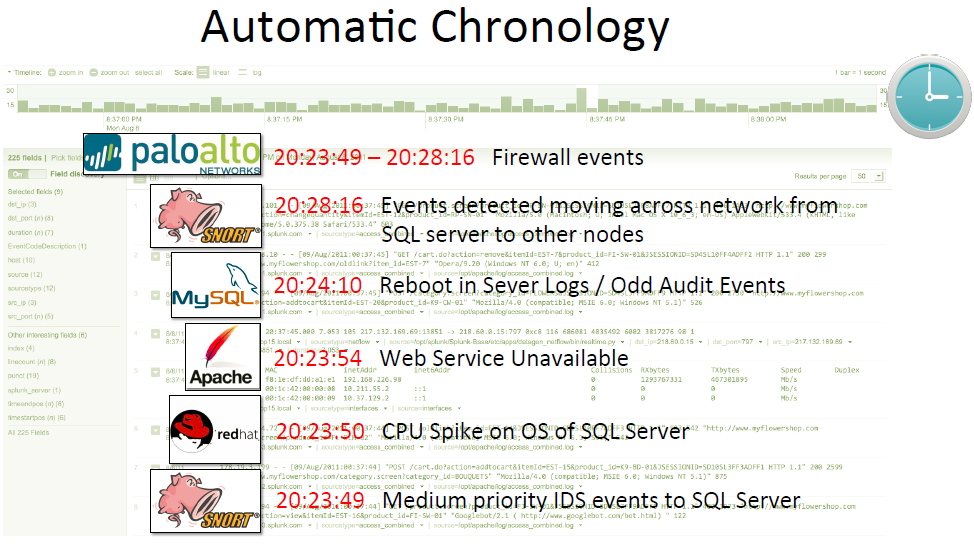
* Search and Alerts
* Tags
* Event Types
* Comparison Operators
* The search pipeline

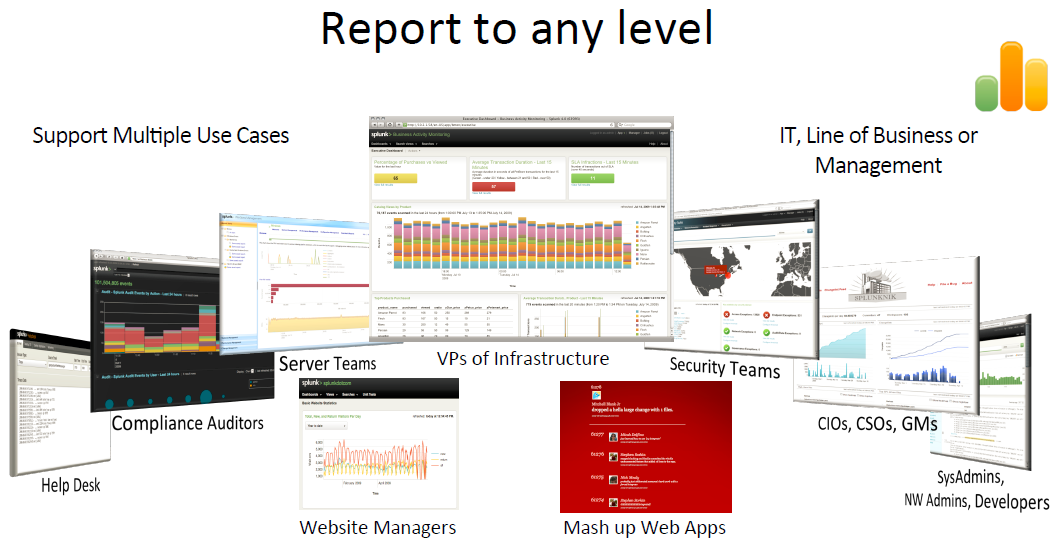
Search>

Search using powerful search language





Search>

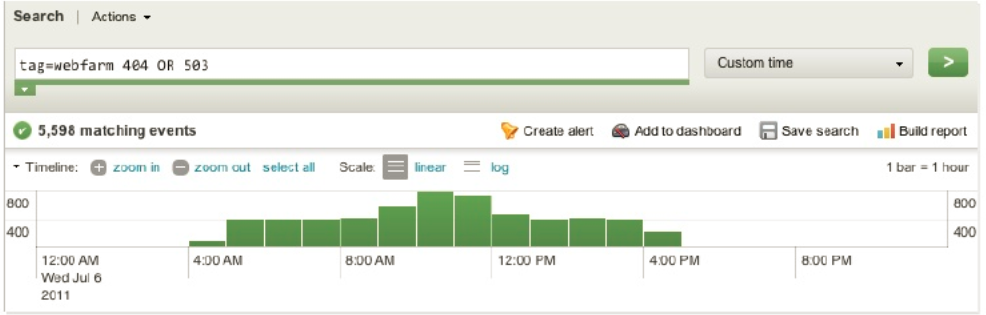


Tags>

Tags are metadata you can add to the search result field



Search tagged item across hosts



Events>

Search into log and save your criteria as event, Event types let you sift through huge amounts of data, find similar patterns, and create alerts and reports.

